IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION
No. 5:19-cv-475-BO

JASON WILLIAMS,
Plaintiff,

v.

AT&T MOBILITY, LLC,
Defendant.

ORDER

This matter is before the Court on defendant's motion to dismiss [DE 14]. For the reasons discussed below, the motion [DE 14] is DENIED.

BACKGROUND

Plaintiff brings this lawsuit against his former wireless carrier, AT&T Mobility, after the company effectuated seven unauthorized reassignments of his SIM card at the behest of hackers.

A SIM ("subscriber identify module") card is a small, removable chip that allows a cell phone to communicate with the wireless carrier and to know which subscriber is associated with that phone. The SIM card associated with a wireless phone can be changed, allowing customers to move their wireless number from one cell phone to another and to continue accessing the carrier network when they switch cell phones. The wireless carrier must effectuate the SIM card reassignment.

A "SIM swap" refers to an unauthorized and illegitimate SIM card change. It is a hacking technique whereby the hacker induces the phone carrier to change the phone associated with the SIM card, rerouting the victim's phone activity (e.g., phone calls, texts) to a third-party phone. The victim loses his or her phone connection while the hacker receives all of the text messages and phone calls intended for the victim. Once the hacker establishes control over the victim's

phone number, he can utilize that number to access the victim's other online accounts, which often utilize phone-based, two-factor authentication for access and password change requests.

Plaintiff's complaint alleges that AT&T effectuated seven unauthorized reassignments of his SIM card between November 5, 2018 and February 8, 2019. These SIM swaps compromised much of his personal and financial data, exposed him and his family to threats to their physical safety, and put aspects of his business at risk. *See* Pl.'s Comp., DE 2. Plaintiff is a co-founder and partner of an asset management company that invests in blockchain technology and digital assets. *Id.* ¶ 8. This included a large-scale bitcoin mining operation, which was discontinued in February 2019 in response to the SIM swaps. *Id.* ¶ 9.

The first SIM swap occurred on November 5, 2018. *Id.* ¶ 37. In the period between when AT&T effectuated the unauthorized change and when plaintiff was able to reverse it, hackers (1) created a mirror image of his phone so that they could see every app; (2) accessed other online accounts, including his Coinbase and Slush Pool accounts;[1] (3) obtained his home address, his and his family members' social security numbers, copies of their passports, TSA precheck information, and financial documents; and (4) threatened to sell his personal information on hacker exchange sites. *Id.* ¶¶ 37–46. The hackers also stole $1,500 worth of bitcoin. *Id.* ¶ 42.

After the attack, plaintiff contacted AT&T to discuss measures the company could take to prevent another SIM swap. *Id.* ¶ 47. AT&T represented that it would add additional security protocols to plaintiff's account. Specifically, AT&T told plaintiff that it would only make SIM card changes in-person at a designated Raleigh AT&T location and that plaintiff would be required to authenticate his identity with two passports. *Id.* Plaintiff also put AT&T on notice that, given his involvement as a cryptocurrency trader, he faced a heightened risk of SIM swap

[1] Coinbase is a cryptocurrency exchange. Slush Pool is a cryptocurrency mining platform.

attacks. *Id.* Relying on AT&T's representations that it was adding these additional safety measures, plaintiff decided not to close his account with the company. *Id.*

The fallout from the first SIM swap was not over, though, because after the attack, the hackers began sending threatening messages to plaintiff. *Id.* ¶ 48. The messages specified his name, home address, and social security number. *Id.* The messages also threatened the physical safety of his family. *Id.*

Despite AT&T's representations that it would not make any SIM card changes outside of the established protocols, the company effectuated a second SIM swap on November 30, 2018, less than a month later. *Id.* ¶ 50. During the hack, plaintiff immediately went to the designated AT&T store with two passports to reverse the change. *Id.* ¶ 52. At the store, he was told that an AT&T employee made the SIM card change at the behest of an impersonator who only provided a fake driver's license as proof of identity. *Id.*

The next day, December 1, 2018, AT&T effected a third unauthorized SIM card change. *Id.* ¶ 53. Plaintiff went to the designated AT&T location the next day, disabled his SIM card, and bought a new iPhone for $700. *Id.* ¶ 57. He purchased the new phone because the AT&T employees represented that it would help mitigate the risk of additional attacks. *Id.* He was again assured that his account was subject to the agreed limitations for changing the SIM card. *Id.* What's more, he was informed that he was on a special list of customers designated as at a high risk for SIM swap attacks. *Id.* ¶ 58.

But that same evening, hours after being assured the company was well aware additional security was needed with respect to his account, AT&T made unauthorized changes to his SIM card a fourth time. *Id.* ¶ 59. With control over his phone number, the hackers accessed his Twitter account and put out messages impersonating him, inducing plaintiff's friends and

associates to send them cryptocurrency. *Id.* ¶ 61. Back at the AT&T store to undo the change, plaintiff asked the employees again to confirm that his account carried special instructions allowing only in-person changes at that location. *Id.* ¶ 64. The employees confirmed the additional protocols. *Id.*

On February 4, 2019, plaintiff was SIM swapped a fifth time. *Id.* ¶ 66. While in control of his phone number, the hackers accessed his accounts on various cryptocurrency exchange platforms. *Id.* ¶ 69. The hackers also accessed his Twitter account again and solicited the exchange of currency from his friends and associates. *Id.* ¶ 70. When he went to the AT&T store the next day, employees informed him the changes had been made to his account in response to an email request and an AT&T online representative changed his four-digit personal identification number ("PIN"). *Id.* ¶ 71.

A sixth unauthorized change to his account was made less than 24 hours later. *Id.* ¶ 72. During this swap, hackers deleted his Slush Pool account, rendering aspects of his business useless. *Id.* ¶ 73. Back at the AT&T store again, two employees helped him get a new SIM card. *Id.* ¶ 74. They also told him that his four-digit PIN had been changed online. *Id.* An AT&T employee made this change to plaintiff's SIM card in response to an over-the-phone request. *Id.* ¶ 75.

Because of this hack and the continued risk that the currency generated through his bitcoin mining operations would be stolen, plaintiff discontinued bitcoin mining. *Id.* ¶ 76. This meant shutting down the activity of 500 computer servers for which he had invested $1.4 million. *Id.* ¶¶ 76–77.

A seventh unauthorized SIM card change was made a few days later. *Id.* ¶ 78. The hackers transferred $6,500 from his bank account to his Coinbase account, which plaintiff is no

longer able to access. *Id.* ¶ 79. Plaintiff went to the designated AT&T store to stop the hack and to notify the company that he was switching carriers. *Id.* ¶ 80. The AT&T employees told him he was ineligible to take his new phone with him to the new carrier. *Id.* Consequently, plaintiff was forced to purchase a new phone from his new carrier. *Id.* ¶ 81.

In response to the seven unauthorized changes and the damage they caused in his life, plaintiff filed this action against AT&T in October 2019. He brings six claims: (1) violation of the Federal Communications Act, 47 U.S.C. § 201 *et seq.*; (2) violation of the North Carolina Unfair and Deceptive Trade Practices Act ("UDTPA"), N.C. Gen. Stat. § 75-1.1; (3) Negligence; (4) Negligent Supervision; (5) violation of North Carolina's computer trespass law, N.C. Gen. Stat. § 1-539.2A; and (6) violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030.

Defendant moves to dismiss the suit pursuant to Federal Rules of Civil Procedure 12(b)(1), 12(b)(6), and 9(b), raising a host of challenges to plaintiff's complaint.

The motion is fully briefed and is ripe for disposition.

DISCUSSION

AT&T challenges the sufficiency of plaintiff's complaint on many fronts. First, the company challenges plaintiff's allegations of proximate cause, arguing that the entire complaint should be dismissed because plaintiff's injuries are (1) unconnected to AT&T's conduct, (2) attributable to plaintiff's own contributory negligence, and (3) attributable to the criminal acts of third parties. AT&T then challenges specific aspects of plaintiff's complaint, arguing: he lacks standing; his UDTPA claim fails to satisfy Federal Rule of Civil Procedure 9(b); his negligence-based claims are barred by the economic loss rule; North Carolina's computer trespass law does

not apply to AT&T; the CFAA claim is inadequately pled; and that plaintiff is not entitled to certain types of relief.

The Court addresses each of AT&T's arguments below. Ultimately, the Court is unpersuaded by any of the company's asserted grounds for dismissal.

I. Plaintiff has standing to sue

At the outset, the Court must address AT&T's argument that plaintiff lacks standing. For an action to constitute a case or controversy under Article III, a "plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016).

Plaintiff easily satisfies these requirements. His complaint is replete with asserted injuries that he personally suffered, including stolen money, deprivation of access to his other online accounts, reputational harm, and experiencing fear in the face of personal threats. These injuries are fairly traceable to AT&T's conduct and would likely be redressed by a favorable decision.

AT&T argues that plaintiff lacks standing because he is seeking to recover on behalf of a business entity for which he is a shareholder. Aside from referring to himself as a "partner," the precise legal structure of plaintiff's business is not specified in the complaint. But the business's legal structure is irrelevant at this juncture as plaintiff clearly has alleged his own injury-in-fact.

II. Plaintiff has properly alleged his claims for relief

"A motion filed under Rule 12(b)(6) challenges the legal sufficiency of a complaint." *Francis v. Giacomelli*, 588 F.3d 186, 192 (4th Cir. 2009). To survive a Rule 12(b)(6) challenge, plaintiff's complaint must articulate facts, that when taken as true, show plaintiff has stated a claim entitling him to relief. *Id.* at 193. The Court need not accept the plaintiff's legal

conclusions drawn from the facts, nor need it accept unwarranted inferences, unreasonable conclusions, or arguments. *Philips v. Pitt County Mem. Hosp.*, 572 F.3d 176, 180 (4th Cir. 2009). "[W]holly vague and conclusory allegations are not sufficient to withstand a motion to dismiss." *Doe v. Virginia Dep't of State Police*, 713 F.3d 745, 754 (4th Cir. 2013).

1. Proximate Cause

AT&T's primary argument for dismissal of the complaint is that plaintiff has failed to allege proximate cause. Specifically, AT&T argues that plaintiff has not alleged a sequence of events connecting AT&T's acts or omissions to the injuries, that plaintiff was contributorily negligent, and that any injuries were based on criminal acts.

"Proximate cause is ordinarily a question of fact for the jury, to be solved by the exercise of good common sense in the consideration of the evidence of each particular case." *Williams v. Carolina Power & Light Co.*, 296 N.C. 400, 403 (1979). A court should only decide proximate cause as a matter of law when reasonable minds cannot possibly differ as to foreseeability of an injury. *Id.*

Defendant's contentions that plaintiff does not connect AT&T's acts or omissions to his injuries and that he was contributorily negligent require little discussion. The complaint chronicles in detail how AT&T repeatedly changed over plaintiff's SIM card without authorization despite plaintiff's constant pleas for the company to follow the security protocols instituted after the first hack. Immediately following each SIM swap, during the intervening period before plaintiff could undo the swap, plaintiff's personal data and online accounts faced an onslaught of hacking attacks, causing the injuries enumerated in the complaint. The connection is clearly stated and is not conclusory. There is also nothing in the complaint suggesting contributory negligence on plaintiff's part.

AT&T also contends plaintiff cannot establish proximate cause as a matter of law because his claims are based on "unforeseeable, independent criminal acts." Def. Resp. at 8.

It is true that, in general, defendants are not liable for the intentional, criminal acts of a third person. *Foster v. Winston-Salem Joint Venture*, 303 N.C. 636, 638 (1981). But this general rule is grounded in foreseeability. *Id.* at 638–39. It is anchored by the theory that intentional criminal acts of third persons cannot be reasonably foreseen. *Id.* Such reasoning is inapplicable here because the SIM swaps were not merely foreseeable by AT&T but were in fact foreseen. As alleged, AT&T swapped plaintiff's SIM card not once, not twice, but seven times. After the first incident the company and plaintiff agreed to specific security protocols because it was aware that he was a high-risk target. On these factual allegations, to hold that proximate is not satisfied as a matter of law because the hackers' conduct is criminal would, in effect, write a new rule immunizing companies from all liability for data breaches. The Court declines to do this.

Moreover, the criminal conduct involved in a SIM swap is not "independent," but is facilitated by the wireless carrier. Unlike a direct hack of data where the company may play a more passive role, SIM swaps are ultimately actualized by the wireless carrier. It is the company that effectuates the SIM card change. This action "remains operative and in force" when the victim's phone activity is used to hack other online accounts, extort the victim, or cause other foreseeable injuries. *Hairston v. Alexander Tank & Equip. Co.*, 310 N.C. 227, 237 (1984) ("In order for the conduct of the intervening agent to break the sequence of events and stay the operative force . . . of the original wrongdoer, the intervening conduct must be of such nature and kind that the original wrongdoer had no reasonable ground to anticipate it[.]").

2. North Carolina Unfair and Deceptive Trade Practice Act

AT&T moves for dismissal of plaintiff's UDTPA claim, arguing that plaintiff failed to satisfy the heightened pleading standards of Federal Rule of Civil Procedure 9(b) for alleged misrepresentations. AT&T also claims plaintiff failed to allege reliance.

Under Rule 9(b), a plaintiff must "describe the time, place, and contents of the false representations, as well as the identity of the person making the misrepresentation and what he obtained thereby." *U.S. ex rel. Wilson v. Kellogg Brown & Root, Inc.*, 525 F.3d 370, 379 (4th Cir. 2008).

The Court finds Rule 9(b) is satisfied and plaintiff has alleged reliance. The complaint alleges that following the first SIM swap on November 5, plaintiff contacted AT&T to discuss adding heightened security measures to his account. Pl.'s Comp. ¶ 47, DE 2. AT&T represented that it added specific protocols to plaintiff's account—SIM card changes could only be made in-person, at a designated store, with identification verified by two passports. *Id.* Plaintiff relied on this assurance and did not close his account. *Id.* From there, plaintiff's complaint details multiple instances of communication with AT&T employees at the designated AT&T store—on November 30, December 2, December 5, February 5, and February 6. In many of these communications, he discussed the specified security protocols with AT&T employees. They repeatedly confirmed the security protocols were listed on his account. In one of these interactions, on December 2, an AT&T employee induced plaintiff to purchase a new iPhone on assurances that it would mitigate his risk of another SIM swap.

In short, plaintiff's complaint clearly enumerates the time, place, and contents of the AT&T's representations to him. It alleges that on specific dates, he went to a specific AT&T store in Raleigh, and spoke with the associates there, who repeatedly reassured him that his SIM

card would not be changed except under very limited circumstances. In reliance, plaintiff kept AT&T as his carrier. AT&T then proceeded to make numerous unauthorized changes to his SIM card, sometimes even changing his PIN as well. While the complaint in some instances specifies the first name of the AT&T employee with whom he interacted, plaintiff cannot reasonably be expected to remember and list the name of each and every employee he dealt with over the course of four months.

The Court is satisfied the requirements of Rule 9(b) are met.

3. Economic Loss Rule

AT&T moves to dismiss plaintiff's negligence and negligent supervision claims under the economic loss rule.

The economic loss rule is designed to prevent plaintiffs from repackaging their breach of contract claims as tort claims. The general rule is that "a breach of contract does not give rise to a tort action by the promisee against the promisor." *N.C. State Ports Auth. v. Lloyd A. Fry Roofing Co.*, 294 N.C. 73, 81 (1978), *rejected in part on other grounds by Trs. of Rowan Tech. Coll. v. J. Hyatt Hammond Assocs., Inc.*, 313 N.C. 230 (1985). There are, however, exceptions to this rule. *Id.* at 82–83. One of those exceptions is that the economic loss rule does not bar tort claims where the promisor's conduct causes damage to "property of the promisee other than the property which was the subject of the contract, or was a personal injury to the promisee[.]" *Ellis v. Louisiana-Pac. Corp.*, 699 F.3d 778, 783 (4th Cir. 2012).

Here, AT&T's alleged negligence led to the compromise of plaintiff's online accounts with other companies, the compromise of legal and financial information, money stolen from his bank account, as well as harm from personal threats and reputational damage. Plaintiff is not seeking to repackage a breach of contract claim for the deficient provision of wireless service.

Rather, he is seeking to recover for tortious conduct where the harms proliferated to every aspect of his life, well beyond his contractual relationship with AT&T. The economic loss rule does not bar his negligence and negligent supervision claims.

4. North Carolina Computer Trespass

Plaintiff brings a claim under N.C. Gen. Stat. § 1-539.2A, which provides a private cause of action to those injured by violation of § 14-458. Section 14-458, North Carolina's criminal trespass statute, makes it unlawful for "any person to use a computer or computer network without authority and with intent to . . . [t]emporarily or permanently remove, halt, or otherwise disable any computer data . . . or cause to be made an unauthorized copy, in any form . . . of computer data[.]" § 14-458(a). "Without authority" means "the person has no right or permission of the owner to use a computer, or the person uses a computer in a manner exceeding the right or permission[.]" *Id.* These provisions do not apply to "[a]ny terms or conditions in a contract or license related to a . . . telecommunication device; or [a]ny software or hardware designed to allow a . . . telecommunication service to operate in the ordinary course of a lawful business[.]" § 14-453.1.

Focusing on the exception's language about telecommunications contracts and service in the ordinary course of business, AT&T argues that it uses its software and hardware to conduct SIM card changes in the ordinary course of business, and therefore, the computer trespass statute does not apply.

The Court disagrees with AT&T's reading of the exception provision. "Statutory rules of construction require the Court to consider the language used in the statute, the mischiefs sought to be avoided, and the remedies intended to be applied." *Appeal of Martin*, 286 N.C. 66, 79 (1974). "[I]f possible, the language of a statute will be interpreted so as to avoid an absurd

consequence." *Id.* (internal quotations omitted). Under AT&T's reading of the exception, business enterprises are incapable of committing computer crimes using their own computer systems because the software and hardware of their systems are always designed for the system to operate in the ordinary course of business.

Here, plaintiff alleges that AT&T violated the statute through its employees, not through its contract terms, hardware, or software. Effectuating an unauthorized SIM card change in a manner that transgresses the explicit permissions of the customer cannot reasonably be said to fall within the ordinary course of lawful business. Given the number of unauthorized SIM card changes, the repeated failures by AT&T to follow the security protocols, and the additional unauthorized changes to his PIN, plaintiff's allegations state a plausible claim that AT&T violated North Carolina's computer trespass law.

5. Computer Fraud and Abuse Act

AT&T argues plaintiff's CFAA claim should be dismissed for failure to plead a qualifying loss. To sustain a private cause of action under CFAA, a plaintiff must allege that defendant's conduct involved at least one of five aggravating factors enumerated in 18 U.S.C. § 1030(g). One of these factors is a "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." § 1030(c)(4)(A)(i)(I).

Plaintiff's complaint clears this $5,000 threshold. He alleges $6,500 was transferred from his bank to his Coinbase account, which he can no longer access. In addition, the complaint plausibly alleges that he spent at least $5,000 in the investigation and remediation of the SIM swaps, including on items like new iPhones, same-day plane tickets to return to North Carolina to rush to the AT&T store, and discontinuing aspects of his business.

6. Damages

Finally, AT&T raises two arguments at the dismissal stage asking the Court to make determinations about the type and scope of relief that is recoverable. First, AT&T asks the Court to dismiss plaintiff's Communications Act claim to the extent it seeks presumed damages, damages for mental or emotional distress, or injunctive relief. Second, AT&T asks the Court to strike plaintiff's prayer for punitive damages, arguing that plaintiff has pleaded no facts that would entitle him to such relief.

The Communications Act states that a "common carrier shall be liable to the person or persons injured thereby for the full amount of damages sustained in consequence of any such violation of the provisions of this chapter[.]" 47 U.S.C. § 206. At least one court of appeals has held that plaintiffs cannot recovery presumed damages under this section. *Conboy v. AT & T Corp.*, 241 F.3d 242, 250–51 (2d Cir. 2001). Presumed damages are damages inferred by law and not specifically proven. *Memphis Cmty. Sch. Dist. v. Stachura*, 477 U.S. 299, 310 (1986). "When a plaintiff seeks compensation for an injury that is likely to have occurred but difficult to establish, some form of presumed damages may possibly be appropriate." *Id.* 310–11.

AT&T erroneously conflates presumed damages and non-economic damages. *Sloane v. Equifax Info. Servs., LLC*, 510 F.3d 495, 500 (4th Cir. 2007) ("Actual damages may include not only economic damages, but also damages for humiliation and mental distress."); *Price v. City of Charlotte, N.C.*, 93 F.3d 1241, 1254 (4th Cir. 1996) (explaining the type of evidence needed to support an award of compensatory damages for emotional distress).

The Court does not read *Conboy*, on which AT&T relies, as holding that damages for emotional distress are precluded under the Communications Act. 241 F.3d at 250–51. Rather, *Conboy* merely rejects the idea that the court should presume damages for emotional distress and

anguish as a matter of law, without evidence. *Id.* The Court is inclined to agree that presumed damages are inappropriate, but the Court need not make such a determination right now as plaintiff's complaint does not appear to rely on presumed damages. Rather, plaintiff alleges substantial actual damages, including financial loss, dissemination of sensitive personal information, reputational damage, and mental anguish.

AT&T's request for the Court to strike the prayer for punitive damages also fails. Under North Carolina law, punitive damages may be awarded against a corporation where "the officers, directors, or managers of the corporation participated in or condoned the conduct constituting the aggravating factor giving rise to punitive damages." N.C. Gen. Stat. § 1D-15. The term "manager" has been interpreted as broadly as "one who conducts, directs, or supervises something." *Everhart v. O'Charley's Inc.*, 200 N.C. App. 142, 153 (2009) (internal quotations omitted). The term is clearly not limited to individuals at the highest level of a company but includes branch or shift managers and the like. *See Everhart*, 200 N.C. App. at 154 (concluding that an assistant dining room manager met the definition of "manager"). Ultimately, whether a "manager" participated or condoned an aggravating factor is a factual determination that is more appropriately left for later. At this stage, plaintiff's complaint states a plausible case that a "manager" was involved in the SIM swaps, which given the special security protocols established, could involve aggravating factors.

CONCLUSION

In sum, the Court concludes that plaintiff has standing and that he has alleged plausible claims for relief under all of his causes of action. For the reasons stated above, defendant's motion to dismiss [DE 14] is DENIED.

SO ORDERED, this 25 day of March, 2020.

TERRENCE W. BOYLE
CHIEF UNITED STATES DISTRICT JUDGE